

FORM PTO-1390 (Modified)
(REV 11-2000)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371

112740-376

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR

10/018272

INTERNATIONAL APPLICATION NO.
PCT/DE00/01650INTERNATIONAL FILING DATE
23 May 2000PRIORITY DATE CLAIMED
15 June 1999

TITLE OF INVENTION

METHOD AND APPARATUS FOR TRANSMITTING DATA

APPLICANT(S) FOR DO/EO/US

Michael Tietsch

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (24) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
 - a. ☒ is attached hereto (required only if not communicated by the International Bureau).
 - b. ☐ has been communicated by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
 - a. ☒ is attached hereto.
 - b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
 - a. ☐ are attached hereto (required only if not communicated by the International Bureau).
 - b. ☐ have been communicated by the International Bureau.
 - c. ☒ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☒ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☒ Certificate of Mailing by Express Mail
23. ☐ Other items or information:

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1.101) 10/018277		INTERNATIONAL APPLICATION NO. PCT/DE00/01650		ATTORNEY'S DOCKET NUMBER 112740-376	
---	--	--	--	---	--

24. The following fees are submitted:				CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) : <input type="checkbox"/> Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO \$1040.00 <input checked="" type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO \$890.00 <input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$740.00 <input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$710.00 <input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) \$100.00 ENTER APPROPRIATE BASIC FEE AMOUNT =				\$890.00	
Surcharge of \$130.00 for furnishing the oath or declaration later than months from the earliest claimed priority date (37 CFR 1.492 (e)). <input type="checkbox"/> 20 <input type="checkbox"/> 30				\$0.00	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	15 - 20 =	0	x \$18.00	\$0.00	
Independent claims	2 - 3 =	0	x \$84.00	\$0.00	
Multiple Dependent Claims (check if applicable). <input type="checkbox"/>				\$0.00	
TOTAL OF ABOVE CALCULATIONS =				\$890.00	
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				\$0.00	
SUBTOTAL =				\$890.00	
Processing fee of \$130.00 for furnishing the English translation later than months from the earliest claimed priority date (37 CFR 1.492 (f)). <input type="checkbox"/> 20 <input type="checkbox"/> 30				\$0.00	
TOTAL NATIONAL FEE =				\$890.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) (check if applicable). <input type="checkbox"/>				\$0.00	
TOTAL FEES ENCLOSED =				\$890.00	
				Amount to be: refunded	\$
				charged	\$

a. ☒ A check in the amount of **\$890.00** to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **02-1818**. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

William E. Vaughan (Reg. No. 39,056)
 Bell, Boyd & Lloyd LLC
 P.O. Box 1135
 Chicago, Illinois 60690-1135

SIGNATURE
 William E. Vaughan
 NAME
 39,056
 REGISTRATION NUMBER
 December 13, 2001
 DATE

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)

Applicant(s): Michael Tietsch

Docket No.

112740-376

Serial No.

Filing Date

Examiner

Group Art Unit

Invention: **METHOD AND APPARATUS FOR TRANSMITTING DATA**

I hereby certify that the following correspondence:

Transmittal letter to the United States Designated/Elected Office in duplicate, International application as originally filed, English translation, Pre Examination Report, Preliminary Amendment, IDS, PTO 1449, executed declaration and power of attorney, filing fee \$890.00, postcard (see enclosed envelope for executed assignment and fee)

(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on

December 13, 2001

(Date)

Robert Buccieri
(Typed or Printed Name of Person Mailing Correspondence)


(Signature of Person Mailing Correspondence)

EL727380876US

("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.

BOX PCT

IN THE UNITED STATES ELECTED/DESIGNATED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY-CHAPTER II

5

PRELIMINARY AMENDMENT

APPLICANT: Michael Tietsch DOCKET NO.: 112740-376
SERIAL NO: GROUP ART UNIT:
FILED: EXAMINER:
INTERNATIONAL APPLICATION NO.: PCT/DE00/01650
INTERNATIONAL FILING DATE 23 May 2000
INVENTION: METHOD AND APPARATUS FOR TRANSMITTING
DATA

Assistant Commissioner for Patents,
Washington, D.C. 20231

10

Sir:

Please amend the above-identified International Application before entry into
the National stage before the U.S. Patent and Trademark Office under 35 U.S.C. §371
as follows:

15 **In the Specification:**

Please replace the Specification of the present application, including the
Abstract, with the following Substitute Specification:

S P E C I F I C A T I O N

TITLE OF THE INVENTION

20

METHOD AND APPARATUS FOR TRANSMITTING DATA

BACKGROUND OF THE INVENTION

The present invention relates to a method for transmitting data from a source
network device to a destination network device. The present invention also relates to
an address conversion apparatus for implementing the method. In this context,
25 network devices can be understood to be network nodes in a communication and/or
data network, router devices, network modules, networked personal computers and
other communication and data processing devices which can be coupled to a network.

In order to switch data quickly within a network, the data are frequently transmitted in the form of data packets provided with a hardware address as destination address. Hardware addresses, which are also referred to as MAC addresses (medium access control), are addresses which are used in the data link layer (layer 2) of the OSI reference model and with which network devices (usually network modules) are provided by the manufacturer. The hardware address for a network device is stored permanently, i.e., unalterably, in the network device and is unique throughout the world.

Switching data packets on the basis of hardware addresses is typical, particularly in local area networks ("LANs"). A data packet which is provided with a hardware address for a destination network device and is sent to a LAN is recognized by the destination network device in question as being addressed to it from the hardware address and is, therefore, received for further processing or forwarding. Normally, hardware addresses are used only for addressing network devices within a local area network. If a transmission destination is situated outside the local area network, the data packets are generally transported to a router device for the local area network, which router device transfers the data packets using a network address which is additionally contained in the data packets and identifies the transmission destination. Unlike a hardware address, a network address is resident above the data link layer and can be reversibly assigned to a network device via system administration. The network addresses used are frequently "Internet Protocol addresses", also referred to as "IP" addresses below. The router device evaluates the network address in the data packets and, on the basis of this, determines an address information item identifying a destination network device which is registered in the router device and is as close as possible to the transmission destination or is possibly identical thereto. The data packets are then transferred to this destination network device using the address information item. If this destination network device does not match the ultimate transmission destination, this destination network device is responsible for transferring the data packets toward the transmission destination.

A method allowing data packets provided with an IP address to be transferred transparently via an ATM network (ATM: asynchronous transfer mode) to a transmission destination which is coupled to the ATM network and is identified by the

10018277 121301
IP address is known by the name IpoA (IP over ATM), for example. In this context, a router device uses the IP address in the data packets to determine the ATM address of an ATM exit network node which is as close as possible to the transmission destination and is used to forward the data packets in the ATM network. Aspects of
5 this method are described in Internet specification RFC 2225, for example.

However, the evaluation of IP addresses for alternate routing which these methods require is a relatively complex operation which can generally be implemented only with a high level of circuit complexity.

It is an object of the present invention, therefore, to specify a method for
10 transmitting data from a source network device to at least one destination network device which requires less complex address evaluation. It is also an aim to specify an address conversion apparatus for implementing the method.

SUMMARY OF THE INVENTION

The inventive method conveys data from a source network device to a
15 destination network device using a fictitious hardware address associated with these data as destination address in the source network device. In this context, the switching on the basis of hardware addresses means that no complex evaluation of network addresses, such as IP addresses, is necessary. The fictitious hardware address referred to in this context is a hardware address information item which the source network
20 device uses, on the basis of a transfer protocol used, to identify a transmission destination without matching the latter's hardware address prescribed by the manufacturer - also referred to below as the real hardware address. To be able, nonetheless, to transfer data associated with a fictitious hardware address to the intended destination network device, an inventive address conversion apparatus is
25 provided. In the latter, fictitious hardware addresses are associated with a respective address information item which identifies a respective destination network device and can be used to convey the data to the respective destination network device.

The direct association between fictitious hardware addresses and address
information items identifying destination network devices in the address conversion
30 apparatus allows an address information item to be determined very easily; e.g., by accessing an association table, using a fictitious hardware address. By contrast, it would be much more difficult to determine such an address information item using an

IP address instead of the fictitious hardware address. Since an IP address refers to a transmission destination at the end of a transfer chain and, in principle, any device provided with an IP address could be addressed throughout the world, there is no point in assigning IP addresses to destination network devices directly. By contrast with
5 this, the number of fictitious hardware addresses to be managed by an inventive address conversion apparatus is limited by the fact that fictitious hardware addresses are provided only for the purpose of addressing transmission destinations registered in the source network device, so that fictitious hardware addresses can be directly assigned to address information items for destination network devices with little
10 memory requirement.

A fundamental advantage of the present invention is that data can also be conveyed, on the basis of hardware addresses, to destination network devices situated outside the local area network of the source network device. To this end, the source network device needs to assign such a destination network device a fictitious hardware
15 address, which the address conversion apparatus in turn assigns an address information item which can be used to convey the data to the destination network device even outside the local area network of the source network device. This significantly extends the range of application for hardware-address based addressing of network devices.

Another fundamental advantage of the present invention can be seen in that changing a real hardware address for a network device, e.g., when replacing a network module, at most requires little reconfiguration effort. This is essentially a consequence of using fictitious hardware addresses. Since these do not need to match any real hardware address for a destination network device, fictitious hardware addresses can
20 also be retained when real hardware addresses are changed. By contrast with this, in the case of the current prior art, any change to a real hardware address for a network device requires that the hardware address tables be updated for all network devices which are meant to be able to address the altered network device using its hardware address.

The address information item associated with a fictitious hardware address in the address conversion apparatus may advantageously be a real hardware address for the destination network device; e.g., the latter's MAC address prescribed by the
30

manufacturer. Data which are associated with a real hardware address and are transferred to the destination network device are recognized by the latter as being addressed to it and are received for the purpose of further processing or forwarding. If the real hardware address of the destination network device changes, e.g., due to a network module being replaced, it is necessary only to change the association between real and fictitious hardware addresses in the address conversion apparatus in order to be able to address the destination network device using the unaltered fictitious hardware address.

Alternatively, the address information item assigned to the data may also be a network address, for example an IP address or an ATM address, for the destination network device. Such a network address also allows addressing of destination network devices which are situated in a different communication network than the source network device.

In accordance with one advantageous embodiment of the present invention, one or more fictitious hardware addresses to be used as destination address can be formed by the address conversion apparatus and transmitted to the source network device. In this context, fictitious hardware addresses need to be formed such that they are unique in the local area network including the source network device and the address conversion apparatus and also do not match any real hardware address in this local area network.

In accordance with another advantageous embodiment of the present invention, an inquiry from the source network device after a hardware address for a network device identified by an address information item contained in the inquiry, e.g., an IP address, can be answered by the address conversion apparatus on behalf of the network device in question. Such inquiries may be made, for example, under the "ARP protocol" (address resolution protocol). For this purpose, the address conversion apparatus transmits a fictitious hardware address associated with this address information item in the address conversion apparatus to the inquiring source network device. This is a simple way of entering fictitious hardware addresses into a hardware address table, used for hardware addressing, associated with the source network device. The fictitious hardware addresses entered are then used for all subsequent data transmissions.

1004837-23007

In accordance with one advantageous embodiment of the present invention, the data to be transferred can be transmitted from the source network device to the destination network device via the address conversion apparatus. As such, the address information item to be used to forward the data to the destination network device can be assigned to the data actually in the address conversion apparatus. In addition, the data can be converted in the address conversion apparatus in line with a transfer protocol used by the destination network device. As such the source network device requires no functionality going beyond the framework of conventional hardware-address based data transmission in order to perform data transmission in accordance with the present invention. The source network device need merely be connected to an inventive address conversion apparatus which can address the destination network device. This allows, by way of example, conventional router devices designed for connecting local area networks directly to be connected to an external communication network, and hence to be coupled to one another, via a respective inventive address conversion apparatus.

Additional features and advantages of the present invention are described in and will be apparent from, the following Detailed Description of the Invention and the Figures.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 shows a schematic illustration of three local area networks coupled via an ATM network.

Figure 2 shows a schematic illustration of two address conversion devices.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 is a schematic illustration of three local area networks LAN1, LAN2 and LAN3 coupled via an ATM network ATM. The local area networks LAN1, LAN2 and LAN3 each include a number of personal computers PC, PCA, PCB coupled locally via Ethernet or FDDI (fiber distributed data interface), for example, and are respectively coupled to the ATM network ATM via a router device R1, R2 or R3. Whereas the router device R1 for the local area network LAN1 and the router device R2 for the local area network LAN2 are respectively connected to the ATM network ATM via an address conversion apparatus A1 or A2, the router device R3 for the local area network LAN3 is connected to the ATM network ATM directly. The

router devices R1 and R2 are conventional router devices which are actually designed for connecting local area networks directly. By contrast, its direct connection to the ATM network ATM means that the router device R3 needs to have not only conventional router functionality but the capability for protocol conversion between a transfer protocol used in the ATM network ATM and a transfer protocol used in the local area network LAN3. The router devices R1, R2 and R3 and also the address conversion apparatuses A1 and A2 are considered to be special embodiments of network devices within the context of the exemplary embodiment.

The router devices R1 and R2 have been assigned a respective MAC address MAC1 and MAC2 as real hardware address by the manufacturer and have been assigned a respective IP address IP1 or IP2 by system administration, in the order specified. The router device R3 has an associated IP address IP3 and, in addition, an ATM address ATM3 as network address. The address conversion apparatuses A1 and A2 also have respectively associated ATM addresses ATM1 or ATM2 as network address. In addition, the personal computer PCB has the associated IP address IPB. The router devices R1, R2 and R3, the address conversion apparatuses A1 and A2 and also the personal computer PCB are respectively uniquely identified by the respectively associated addresses MAC1, MAC2, IP1, IP2, IP3, IPB, ATM1, ATM2 and ATM3.

Figure 2 shows a schematic illustration of the address conversion apparatuses A1 and A2 via which the router devices R1 and R2 are coupled to the ATM network ATM. The address conversion apparatuses A1 and A2 each contain, as functional components, a central controller ZS including a protocol conversion apparatus PU, an address assignment device AZ, an address determination device AE and an address checking device AP, and also an association table memory ZT which can be accessed by the central controller ZS. In both address conversion apparatuses A1 and A2, the protocol conversion apparatus PU and the address assignment device AZ, and the address determination device AE and the address checking device AP, are respectively produced in a joint module.

In this exemplary embodiment, the association table memories ZT in the address conversion apparatuses A1 and A2 each contain at least three entries, in accordance with the number of local area networks LAN1, LAN2 and LAN3 coupled.

The association table memory ZT in the address conversion apparatus A1 contains a first entry with the IP address IP1, the MAC address MAC1 and the ATM address ATM1, a second entry with the IP address IP2, a fictitious MAC address FIMAC2 and the ATM address ATM2, and also a third entry with the IP address IP3, a fictitious
5 MAC address FIMAC3 and the ATM address ATM3.

The association table memory ZT in the address conversion apparatus A2 correspondingly contains a first entry with the IP address IP2, the MAC address MAC2 and the ATM address ATM2, a second entry with the IP address IP1, a fictitious MAC address FIMAC4 and the ATM address ATM1, and also a third entry
10 with the IP address IP3, a fictitious MAC address FIMAC5 and the ATM address ATM3. In this context, the elements of each entry are respectively stored associated with one another.

The fictitious MAC addresses FIMAC1, FIMAC2, FIMAC4 and FIMAC5 each have the format of a hardware address. The fictitious MAC address FIMAC2 or
15 FIMAC3 is used by the router device R1 to address the router device R2 or R3, and the fictitious MAC address FIMAC4 or FIMAC5 is used by the router device R2 to address the router device R1 or R3. To this end, the fictitious MAC addresses FIMMAC2, FIMAC3 are entered into a routing table (not shown) for the router device R1, and the fictitious MAC addresses FIMAC4, FIMAC5 are entered into a routing
20 table (not shown) for the router device R2. The fictitious MAC addresses FIMAC1, FIMAC2, FIMAC4 and FIMAC5 are fictitious insofar as they match none of the real hardware addresses MAC1 and MAC2, prescribed by the manufacturer, of the router devices R1 and R2 which they address, or they are not based on any real hardware address as in the case of the router device R3. Nevertheless, the fictitious MAC
25 addresses are treated as real MAC addresses from the point of view of the router devices R1 and R2.

The fictitious MAC addresses FIMAC2, FIMAC3 and FIMAC4, FIMAC5 are entered into the routing tables for the router devices R1 and R2 by the address conversion apparatuses A1 and A2 under the "ARP" protocol (address resolution
30 protocol). Under this ARP protocol, inquiries from the router device R1 or R2 after MAC addresses for network devices are answered by the address conversion apparatus A1 or A2 on behalf of these network devices. In the course of such a request, the

inquiring router device R1 or R2 transfers an IP address to the connected network devices with the order to send the MAC address of the network device identified by the IP address to the router device R1 or R2, if known. By way of example, such an inquiry after the MAC address of the router device R2 identified by the IP address IP2
5 may be transmitted from the router device R1 to the address conversion apparatus A1. In such a case, the address conversion apparatus A1 first checks whether the IP address transferred with the inquiry, in this case IP2, is held in the association table memory ZT. If it is, the inquiry is answered by the address conversion apparatus A1 by sending the MAC address associated with this IP address in the association table
10 memory ZT, in this case the fictitious MAC address FIMAC2, to the inquiring router device R1. The fictitious MAC address FIMAC2 transmitted to the router device R1 is then entered by the router device R1 into its routing table as MAC address for the router device R2. Inquiries from the router device R2 are answered by the address conversion apparatus A2 in a similar manner.

15 The fact that such inquiries are answered on a delegated basis by fictitious MAC addresses FIMAC2, FIMAC3 and FIMAC4, FIMAC5 stored in the address conversion apparatuses A1 and A2 allows for the real hardware addresses MAC1, MAC2 no longer to be obtained in a complex manner via the communication network ATM. It also becomes unnecessary for each change to a real hardware address for a
20 router device coupled via the ATM network ATM, e.g., as a result of a network module being replaced, to involve the routing tables for all other router devices being updated.

The text below considers data being conveyed on the basis of hardware addresses between the local area networks LAN1, LAN2, LAN3 using the example of
25 data transmission from the local area network LAN1 to the local area network LAN2.

To transmit data from the personal computer PCA situated in the local area network LAN1 to the destination personal computer PCB situated in the local area network LAN2, the data are transmitted to the router device R1 in the form of data packets containing the IP address IPB of the destination personal computer PCB. The
30 router device R1 uses the routing table it contains to ascertain that the destination personal computer PC2 identified by the IP address IPB can be reached via the router device R2. Consequently, the router device R1 provides the data packets to be

transmitted with the fictitious MAC address FIMAC2 obtained from the address conversion apparatus A1 as the hardware address for the router device R2. The IP address IPB of the destination personal computer PCB is maintained unaltered in the data packets in this context. The data packets are then forwarded from the router device R1 to the address conversion apparatus A1.

In the address conversion apparatus A1, the address checking device AP first checks whether the fictitious MAC address FIMAC2 received is held in the association table memory ZT. If it is, the address determination device PE determines the ATM address associated with the fictitious MAC address FIMAC2 in the association table memory ZT (in this case ATM2), which ATM address identifies that address conversion apparatus A2 via which the router device R2 is coupled to the ATM network ATM. The data packets to be transmitted are then converted by the protocol conversion apparatus PU, in line with the transfer protocol used in the ATM network ATM, into ATM cells to which the ATM address ATM2 is assigned as network address by the address assignment device AZ. The ATM cells are then forwarded to the ATM network ATM and are transferred therefrom to the address conversion apparatus A2 identified by the ATM address ATM2. In this context, the ATM cells may be transferred both via one or more fixed connections (PVC: permanent virtual circuit) and via one or more switched connections (SVC: switched virtual circuit) to be set up as required in the ATM network ATM.

The address conversion apparatus A2 converts the ATM cells into data packets in line with the IP protocol again, the data packets being provided with the real MAC address MAC2 of the router device R2, which is held in the association table memory ZT in this address conversion apparatus A2. The data packets are then forwarded to the router device R2, which recognizes the data packets as being addressed to it from the real MAC address MAC2 associated with them. The router device R2 then forwards the data packets received, after evaluating their IP address IPB, to the destination personal computer PCB identified by the IP address IPB.

Data packets are transferred from the local area network LAN1 to a destination personal computer PC situated in the local area network LAN3 in a largely similar manner, with the difference that, in this case, the data packets are addressed to the router device R3 directly using the ATM address ATM3. The router device R3

therefore needs to have both protocol conversion functionality and routing functionality.

In the present exemplary embodiment, fictitious MAC addresses are effective only for communication between a router device and the respective address conversion apparatus connected directly thereto. In this context, a router device and the address conversion apparatus connected directly thereto form a separate local area network. Hence, the fictitious MAC addresses FIMAC2, FIMAC3 of the address conversion apparatus A1 can be used independently of the fictitious MAC addresses FIMAC4, FIMAC5 of the address conversion apparatus A2. In particular, the fictitious MAC addresses FIMAC2 and FIMAC3 used by the address conversion apparatus A1 can match the fictitious MAC addresses FIMAC4 and FIMAC5 used by the address conversion apparatus A2. Fictitious MAC addresses can therefore be formed in an address conversion apparatus or assigned by system administration independently of the fictitious MAC addresses of another address conversion apparatus.

To allow a router device R1 or R2 to address network devices uniquely using fictitious MAC addresses, these MAC addresses need to be unique within the local area network formed by the router device and the address conversion apparatus connected directly thereto. In particular, a fictitious MAC address must not match any real or other fictitious MAC address in this local area network. This may be ensured, by way of example, by allocating real MAC addresses of old network devices no longer in use as fictitious MAC addresses. Alternatively, fictitious MAC addresses may be taken from a contingent reserved only for this purpose. Since fictitious MAC addresses can be repeated in different local area networks, this requires the provision of only one contingent within the scope of an appropriate maximum size for a local area network. The measures cited ensure that no conflict arises between a fictitious MAC address and a real MAC address even when real MAC addresses are changed within the local area network; e.g., due to a network module being replaced.

Although the present invention has been described with reference to specific embodiments, those of skill in the art will recognize that changes may be made thereto without departing from the spirit and scope of the invention as set forth in the hereafter appended claims.

In the claims:

On page 15, cancel line 1 and substitute the following left-hand justified heading therefore.

CLAIMS

5 Please cancel claims 1-15, without prejudice, and substitute the following claims therefore:

16. A method for transmitting data from a source network device to a destination network device, the method comprising the steps of:

10 assigning the data, via the source network device, a fictitious hardware address as destination address, the fictitious hardware address being a hardware address information item which the source network device uses, based on a transfer protocol used, to identify a transmission destination without matching a manufacturer-prescribed hardware address of the transmission destination;

15 transmitting the fictitious hardware address from the source network device to an address conversion apparatus;

 checking, via the address conversion apparatus, whether the transmitted fictitious hardware address matches a stored fictitious hardware address stored in a memory of the address conversion apparatus;

20 assigning the data an address information item, if a result of the check is positive, which is associated with the transmitted fictitious hardware address in the address conversion apparatus;

 identifying, via the address information item, the destination network device ;
and

25 using the address information item to forward the data to the destination network device.

17. A method for transmitting data from a source network device to a destination network device as claimed in Claim 16, wherein the address information item assigned to the data is a real hardware address for the destination network device.

30

18. A method for transmitting data from a source network device to a destination network device as claimed in Claim 16, wherein the address information item assigned to the data is a network address for the destination network device.

5 19. A method for transmitting data from a source network device to a destination network device as claimed in Claim 16, wherein the fictitious hardware address used as the destination address is formed by the address conversion apparatus and is transmitted to the source network device.

10 20. A method for transmitting data from a source network device to a destination network device as claimed in Claim 16, the method further comprising the steps of:

answering an inquiry from the source network device, after a hardware address for a network device identified by an address information item contained in the
15 inquiry, by the address conversion apparatus; and

transmitting to the source network device via the address conversion apparatus, a fictitious hardware address associated with the address information item in question.

20 21. A method for transmitting data from a source network device to a destination network device as claimed in Claim 20, wherein the address information item contained in the inquiry is a network address.

22. A method for transmitting data from a source network device to a destination network device as claimed in Claim 16, wherein the hardware address is an
25 MAC address.

23. A method for transmitting data from a source network device to a destination network device as claimed in Claim 16, wherein the data are transmitted from the source network device to the destination network device via the address
30 conversion apparatus.

24. A method for transmitting data from a source network device to a destination network device as claimed in Claim 23, wherein the data are converted in

the address conversion apparatus in line with a transfer protocol used by the destination network device.

25. An address conversion apparatus for converting fictitious hardware addresses into address information items identifying at least one destination network device, the fictitious hardware address being a hardware address information item which a source network device uses, based on a transfer protocol used, to identify a transmission destination without matching a manufacturer-prescribed hardware address of the transmission destination, the apparatus comprising:

an association table memory in which at least one fictitious hardware address is stored associated with a respective address information item which identifies a destination network device;

an address checking device for checking whether a fictitious hardware address coming from the source network device matches a fictitious hardware address stored in the association table memory; and

an address determination device for determining the address information item associated with a fictitious hardware address which comes from the source network device and is stored in the association table memory.

26. An address conversion apparatus as claimed in Claim 25, further comprising:

an address assignment device for assigning data which come from the source network device and are associated with a respective fictitious hardware address to an address information item associated with the respective fictitious hardware address in the association table memory.

27. An address conversion device as claimed in claim 26, further comprising a protocol conversion apparatus for converting the data coming from the source network device in line with a transfer protocol used by the destination network device.

28. An address conversion apparatus as claimed in claim 25, further comprising a device for forming fictitious hardware addresses to be used as destination addresses.

5 29. An address conversion apparatus as claimed in claim 25, further comprising an address resolution device for answering inquiries from the source network device after a hardware address for a network device, which is identified by an address information item contained in the inquiry, by looking up the fictitious hardware address associated with the address information item in the association table
10 memory and transmitting it to the source network device.

30. An address conversion device as claimed in one claim 25, further comprising a part for entering address information items into the association table memory.

TO BE EXAMINED

ABSTRACT OF THE DISCLOSURE

A method and apparatus for transmitting data wherein it is possible to transmit data on the basis of hardware addresses from a source network device to a destination network device. The source network device assigns the data to be transmitted a fictitious hardware address which is used to identify a transmission destination without matching the latter's real hardware address prescribed by the manufacturer. The fictitious hardware address is transferred to an inventive address conversion apparatus in which the fictitious hardware address has been assigned an address information item identifying the destination network device. The address information item associated with the fictitious hardware address is then assigned to the data, which are forwarded to the destination network device using this address information item.

REMARKS

The present amendment makes editorial changes and corrects typographical errors in the specification, which includes the Abstract, in order to conform the specification to the requirements of United States Patent Practice. No new matter is added thereby. Attached hereto is a marked-up version of the changes made to the specification by the present amendment. The attached page is captioned "**Version With Markings To Show Changes Made**".

In addition, the present amendment cancels original claims 1-15 in favor of new claims 16-30. Claims 16-30 have been presented solely because the revisions by red-lining and underlining which would have been necessary in claims 1-15 in order to present those claims in accordance with preferred United States Patent Practice would have been too extensive, and thus would have been too burdensome. The present amendment is intended for clarification purposes only and not for substantial reasons related to patentability pursuant to 35 U.S.C. §§101, 102, 103 or 112. Indeed, the cancellation of claims 1-15 does not constitute an intent on the part of the Applicants to surrender any of the subject matter of claims 1-15.

Early consideration on the merits is respectfully requested.

Respectfully submitted,



(Reg. No. 39,056)
William E. Vaughan
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690-1135
(312) 807-4292
Attorneys for Applicants

VERSIONS WITH MARKINGS TO SHOW CHANGES MADE

In The Specification:

The Specification of the present application, including the Abstract, has been amended as follows:

5 Description

SPECIFICATION

~~Method and device for transmitting data~~

TITLE OF THE INVENTION

METHOD AND APPARATUS FOR TRANSMITTING DATA

10

BACKGROUND OF THE INVENTION

The present invention relates to a method for transmitting data from a source network device to a destination network device. The present invention also relates to an address conversion ~~device~~ apparatus for implementing the method. In this context, network devices can be understood to ~~mean~~ be network nodes in a communication and/or data network, router devices, network modules, networked personal computers and other communication and data processing devices which can be coupled to a network.

In order to switch data quickly within a network, the data are frequently transmitted in the form of data packets provided with a hardware address as destination address. Hardware addresses, which are also referred to as MAC addresses (medium access control), are addresses which are used in the data link layer (layer 2) of the OSI reference model and with which network devices -(usually network modules-) are provided by the manufacturer. The hardware address for a network device is stored permanently, i.e., unalterably, in the network device and is unique throughout the world.

Switching data packets on the basis of hardware addresses is ~~usual~~ typical, particularly in local area networks ("LANs"). A data packet which is provided with a hardware address for a destination network device and is sent to a LAN is recognized by the destination network device in question as being addressed to it from the hardware address; and is, therefore, received for further processing or forwarding. Normally, hardware addresses are used only for addressing network devices within a local area network. If a transmission destination is situated outside the local area

network, the data packets are generally transported to a router device for the local area network, which router device transfers the data packets using a network address which is additionally contained in ~~said~~ the data packets and identifies the transmission destination. Unlike a hardware address, a network address is resident above the data link layer and can be reversibly assigned to a network device ~~by means of~~ via system administration. The network addresses used are frequently "Internet Protocol addresses", also referred to as "IP" addresses below. The router device evaluates the network address in the data packets and, on the basis of this, determines an address information item identifying a destination network device which is registered in the router device and is as close as possible to the transmission destination or is possibly identical thereto. The data packets are then transferred to this destination network device using the address information item. If this destination network device does not match the ultimate transmission destination, this destination network device is responsible for transferring the data packets toward the transmission destination.

A method allowing data packets provided with an IP address to be transferred transparently via an ATM network (ATM: asynchronous transfer mode) to a transmission destination which is coupled to the ATM network and is identified by the IP address is known by the name IpoA (IP over ATM), for example. In this context, a router device uses the IP address in the data packets to determine the ATM address of an ATM exit network node which is as close as possible to the transmission destination and is used to forward the data packets in the ATM network. Aspects of this method are described in Internet specification RFC 2225, for example.

However, the evaluation of IP addresses for alternate routing which these methods require is a relatively complex operation which can generally be implemented only with a high level of circuit complexity.

It is an object of the present invention, therefore, to specify a method for transmitting data from a source network device to at least one destination network device which requires less complex address evaluation. It is also an aim to specify an address conversion device apparatus for implementing the method.

~~This object is achieved by a method having the features of patent claim 1 and by an address conversion device having the features of patent claim 10.~~

SUMMARY OF THE INVENTION

The inventive method conveys data from a source network device to a destination network device using a fictitious hardware address associated with these data as destination address in the source network device. In this context, the switching on the basis of hardware addresses means that no complex evaluation of network addresses, such as IP addresses, is necessary. The fictitious hardware address referred to in this context is a hardware address information item which the source network device uses, on the basis of a transfer protocol used, to identify a transmission destination without matching the latter's hardware address prescribed by the manufacturer - also referred to below as the real hardware address. To be able, nonetheless, to transfer data associated with a fictitious hardware address to the intended destination network device, an inventive address conversion device apparatus is provided. In the latter, fictitious hardware addresses are associated with a respective address information item which identifies a respective destination network device and can be used to convey the data to the respective destination network device.

The direct association between fictitious hardware addresses and address information items identifying destination network devices in the address conversion device apparatus allows an address information item to be determined very easily; e.g., by accessing an association table, using a fictitious hardware address. By contrast, it would be much more difficult to determine such an address information item using an IP address instead of the fictitious hardware address. Since an IP address refers to a transmission destination at the end of a transfer chain, and, in principle, any device provided with an IP address could be addressed throughout the world, there is no point in assigning IP addresses to destination network devices directly. By contrast with this, the number of fictitious hardware addresses to be managed by an inventive address conversion device apparatus is limited by the fact that fictitious hardware addresses are provided only for the purpose of addressing transmission destinations registered in the source network device, so that fictitious hardware addresses can be directly assigned to address information items for destination network devices with little memory requirement.

A fundamental advantage of the present invention is that data can also be conveyed, on the basis of hardware addresses, to destination network devices situated

outside the local area network of the source network device. To this end, the source network device needs to assign such a destination network device a fictitious hardware address, which the address conversion device apparatus in turn assigns an address information item which can be used to convey the data to the destination network device even outside the local area network of the source network device. This significantly extends the range of application for hardware-address based addressing of network devices.

Another fundamental advantage of the present invention can be seen in that changing a real hardware address for a network device, e.g., when replacing a network module, at most requires little reconfiguration effort. This is essentially a consequence of using fictitious hardware addresses. Since these do not need to match any real hardware address for a destination network device, fictitious hardware addresses can also be retained when real hardware addresses are changed. By contrast with this, in the case of the current prior art, any change to a real hardware address for a network device requires that the hardware address tables be updated for all network devices which are meant to be able to address the altered network device using its hardware address.

~~Advantageous embodiments and developments of the invention are specified in the subclaims.~~

The address information item associated with a fictitious hardware address in the address conversion device apparatus may advantageously be a real hardware address for the destination network device; e.g., the latter's MAC address prescribed by the manufacturer. Data which are associated with a real hardware address and are transferred to the destination network device are recognized by the latter as being addressed to it and are received for the purpose of further processing or forwarding. If the real hardware address of the destination network device changes, e.g. ~~on account of~~ due to a network module being replaced, it is necessary only to change the association between real and fictitious hardware addresses in the address conversion device apparatus in order to be able to address the destination network device using the unaltered fictitious hardware address.

Alternatively, the address information item assigned to the data may also be a network address, for example an IP address or an ATM address, for the destination

network device. Such a network address also allows addressing of destination network devices which are situated in a different communication network than the source network device.

5 In accordance with one advantageous ~~development~~ embodiment of the present invention, one or more fictitious hardware addresses to be used as destination address can be formed by the address conversion ~~device~~ apparatus and transmitted to the source network device. In this context, fictitious hardware addresses need to be formed such that they are unique in the local area network ~~comprising~~ including the source network device and the address conversion ~~device~~ apparatus and also do not
10 match any real hardware address in this local area network.

In accordance with another advantageous ~~development~~ embodiment of the present invention, an ~~enquiry~~ inquiry from the source network device after a hardware address for a network device identified by an address information item contained in the ~~enquiry~~, inquiry, e.g., an IP address, can be answered by the address conversion
15 ~~device~~ apparatus on behalf of the network device in question. Such ~~enquiries~~ inquiries may be made, for example, under the “ARP protocol” (address resolution protocol). For this purpose, the address conversion ~~device~~ apparatus transmits a fictitious hardware address associated with this address information item in the address conversion ~~device~~ apparatus to the ~~enquiring~~ inquiring source network device. This is
20 a simple way of entering fictitious hardware addresses into a hardware address table, used for hardware addressing, associated with the source network device. The fictitious hardware addresses entered are then used for all subsequent data transmissions.

In accordance with one advantageous embodiment of the present invention, the
25 data to be transferred can be transmitted from the source network device to the destination network device via the address conversion ~~device~~. ~~This means that~~ apparatus. As such, the address information item to be used to forward the data to the destination network device can be assigned to the data actually in the address conversion ~~device~~ apparatus. In addition, the data can be converted in the address
30 conversion ~~device~~ apparatus in line with a transfer protocol used by the destination network device. ~~This means that~~ As such the source network device requires no functionality going beyond the framework of conventional hardware-address based

data transmission in order to perform data transmission in accordance with the present invention. The source network device need merely be connected to an inventive address conversion device apparatus which can address the destination network device. This allows, by way of example, conventional router devices designed for
5 connecting local area networks directly to be connected to an external communication network, and hence to be coupled to one another, via a respective inventive address conversion ~~device.~~ apparatus.

~~An exemplary embodiment of the invention is explained in more detail below with reference to the drawing.~~ Additional features and advantages of the present
10 invention are described in and will be apparent from, the following Detailed Description of the Invention and the Figures.

BRIEF DESCRIPTION OF THE FIGURES

~~In the drawing, figure~~ Figure 1 shows a schematic illustration of three local
15 area networks coupled via an ATM network, ~~and.~~

figure Figure 2 shows a schematic illustration of two address conversion devices.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 is a schematic illustration of three local area networks LAN1, LAN2
20 and LAN3 coupled via an ATM network ATM. The local area networks LAN1, LAN2 and LAN3 each ~~comprise a plurality~~ include a number of personal computers PC, PCA, PCB coupled locally ~~by means of~~ via Ethernet or FDDI (fiber distributed data interface), for example, and are respectively coupled to the ATM network ATM via a router device R1 ~~or~~, R2 or R3. Whereas the router device R1 for the local area
25 network LAN1 and the router device R2 for the local area network LAN2 are respectively connected to the ATM network ATM via an address conversion ~~device~~ apparatus A1 or A2, the router device R3 for the local area network LAN3 is connected to the ATM network ATM directly. The router devices R1 and R2 are conventional router devices which are actually designed for connecting local area
30 networks directly. By contrast, its direct connection to the ATM network ATM means that the router device R3 needs to have not only conventional router functionality but ~~also means~~ the capability for protocol conversion between a transfer protocol used in

the ATM network ATM and a transfer protocol used in the local area network LAN3. The router devices R1, R2 and R3 and also the address conversion devices apparatuses A1 and A2 are considered to be special embodiments of network devices within the context of the exemplary embodiment.

5 The router devices R1 and R2 have been assigned a respective MAC address MAC1 and MAC2 as real hardware address by the manufacturer and have been assigned a respective IP address IP1 or IP2 by system administration, in the order specified. The router device R3 has an associated IP address IP3 and, in addition, an ATM address ATM3 as network address. The address conversion devices apparatuses
10 A1 and A2 also have ~~a respective~~ respectively associated ATM ~~address~~ addresses ATM1 or ATM2 as network address. In addition, the personal computer PCB has the associated IP address IPB. The router devices R1, R2 and R3, the address conversion devices apparatuses A1 and A2 and also the personal computer PCB are respectively uniquely identified by the respectively associated addresses MAC1, MAC2, IP1, IP2,
15 IP3, IPB, ATM1, ATM2 and ATM3.

Figure 2 shows a schematic illustration of the address conversion devices apparatuses A1 and A2 via which the router devices R1 and R2 are coupled to the ATM network ATM. The address conversion devices apparatuses A1 and A2 each contain, as functional components, a central controller ZS ~~comprising~~ including a
20 protocol conversion device apparatus PU, an address assignment device AZ, an address determination device AE and an address checking device AP, and also an association table memory ZT which can be accessed by the central controller ZS. In both address conversion devices apparatuses A1 and A2, the protocol conversion device apparatus PU and the address assignment device AZ, and the address
25 determination device AE and the address checking device AP, are respectively produced in a joint module.

In this exemplary embodiment, the association table memories ZT in the address conversion devices apparatuses A1 and A2 each contain at least three entries, in accordance with the number of local area networks LAN1, LAN2 and LAN3
30 coupled. The association table memory ZT in the address conversion device apparatus A1 contains a first entry with the IP address IP1, the MAC address MAC1 and the ATM address ATM1, a second entry with the IP address IP2, a fictitious MAC address

FIMAC2 and the ATM address ATM2, and also a third entry with the IP address IP3, a fictitious MAC address FIMAC3 and the ATM address ATM3.

The association table memory ZT in the address conversion ~~device~~ apparatus A2 correspondingly contains a first entry with the IP address IP2, the MAC address MAC2 and the ATM address ATM2, a second entry with the IP address IP1, a fictitious MAC address FIMAC4 and the ATM address ATM1, and also a third entry with the IP address IP3, a fictitious MAC address FIMAC5 and the ATM address ATM3.

In this context, the elements of each entry are respectively stored associated with one another.

The fictitious MAC addresses FIMAC1, FIMAC2, FIMAC4 and FIMAC5 each have the format of a hardware address. The fictitious MAC address FIMAC2 or FIMAC3 is used by the router device R1 to address the router device R2 or R3, and the fictitious MAC address FIMAC4 or FIMAC5 is used by the router device R2 to address the router device R1 or R3. To this end, the fictitious MAC addresses FIMAC2, FIMAC3 are entered into a routing table (not shown) for the router device R1, and the fictitious MAC addresses FIMAC4, FIMAC5 are entered into a routing table (not shown) for the router device R2. The fictitious MAC addresses FIMAC1, FIMAC2, FIMAC4 and FIMAC5 are fictitious insofar as they match none of the real hardware addresses MAC1 and MAC2, prescribed by the manufacturer, of the router devices R1 and R2 which they address, or they are not based on any real hardware address -as in the case of the router device R3. Nevertheless, the fictitious MAC addresses are treated as real MAC addresses from the point of view of the router devices R1 and R2.

The fictitious MAC addresses FIMAC2, FIMAC3 and FIMAC4, FIMAC5 are entered into the routing tables for the router devices R1 and R2 by the address conversion ~~devices~~ apparatus A1 and A2 under the "ARP" protocol (address resolution protocol). Under this ARP protocol, ~~enquiries~~ inquiries from the router device R1 or R2 after MAC addresses for network devices are answered by the address conversion ~~device~~ apparatus A1 or A2 on behalf of these network devices. In the course of such a request, the ~~enquiring~~ inquiring router device R1 or R2 transfers an IP address to the connected network devices with the order to send the MAC address of the network

device identified by the IP address to the router device R1 or R2, if known. By way of example, such an enquiry inquiry after the MAC address of the router device R2 identified by the IP address IP2 may be transmitted from the router device R1 to the address conversion ~~device~~ apparatus A1. In such a case, the address conversion ~~device~~ apparatus A1 first checks whether the IP address transferred with the enquiry inquiry,
5 apparatus A1 first checks whether the IP address transferred with the enquiry inquiry, in this case IP2, is held in the association table memory ZT. If it is, the enquiry inquiry is answered by the address conversion ~~device~~ apparatus A1 by sending the MAC address associated with this IP address in the association table memory ZT, in this case the fictitious MAC address FIMAC2, to the ~~enquiring~~ inquiring router device
10 R1. The fictitious MAC address FIMAC2 transmitted to the router device R1 is then entered by the router device R1 into its routing table as MAC address for the router device R2. Enquiries Inquiries from the router device R2 are answered by the address conversion ~~device~~ apparatus A2 in a similar manner.

The fact that such enquiries inquiries are answered on a delegated basis by
15 fictitious MAC addresses FIMAC2, FIMAC3 and FIMAC4, FIMAC5 stored in the address conversion ~~devices~~ apparatuses A1 and A2 ~~means that~~ allows for the real hardware addresses MAC1, MAC2 no longer ~~need~~ to be obtained in a complex manner via the communication network ATM. It also becomes unnecessary for each change to a real hardware address for a router device coupled via the ATM network
20 ATM, e.g., as a result of a network module being replaced, ~~also~~ to involve the routing tables for all other router devices being updated.

The text below considers data being conveyed on the basis of hardware addresses between the local area networks LAN1, LAN2, LAN3 using the example of data transmission from the local area network LAN1 to the local area network LAN2.

25 To transmit data from the personal computer PCA situated in the local area network LAN1 to the destination personal computer PCB situated in the local area network LAN2, the data are transmitted to the router device R1 in the form of data packets containing the IP address IPB of the destination personal computer PCB. The router device R1 uses the routing table it contains to ascertain that the destination
30 personal computer PC2 identified by the IP address IPB can be reached via the router device R2. Consequently, the router device R1 provides the data packets to be transmitted with the fictitious MAC address FIMAC2 obtained from the address

conversion ~~device~~ apparatus A1 as the hardware address for the router device R2. The IP address IPB of the destination personal computer PCB is maintained unaltered in the data packets in this context. The data packets are then forwarded from the router device R1 to the address conversion ~~device~~ apparatus A1.

5 In the address conversion ~~device~~ apparatus A1, the address checking device AP first checks whether the fictitious MAC address FIMAC2 received is held in the association table memory ZT. If it is, the address determination device PE determines the ATM address associated with the fictitious MAC address FIMAC2 in the association table memory ZT -(in this case ATM2-), which ATM address identifies
10 that address conversion ~~device~~ apparatus A2 via which the router device R2 is coupled to the ATM network ATM. The data packets to be transmitted are then converted by the protocol conversion ~~device~~ apparatus PU, in line with the transfer protocol used in the ATM network ATM, into ATM cells to which the ATM address ATM2 is assigned as network address by the address assignment device AZ. The ATM cells are then
15 forwarded to the ATM network ATM and are transferred therefrom to the address conversion ~~device~~ apparatus A2 identified by the ATM address ATM2. In this context, the ATM cells may be transferred both via one or more fixed connections (PVC: permanent virtual circuit) and via one or more switched connections (SVC: switched virtual circuit) to be set up as required in the ATM network ATM.

20 The address conversion ~~device~~ apparatus A2 converts the ATM cells into data packets in line with the IP protocol again, said the data packets being provided with the real MAC address MAC2 of the router device R2, which is held in the association table memory ZT in this address conversion ~~device~~ apparatus A2. The data packets are then forwarded to the router device R2, which recognizes the data packets as being
25 addressed to it from the real MAC address MAC2 associated with them. The router device R2 then forwards the data packets received, after evaluating their IP address IPB, to the destination personal computer PCB identified by the IP address IPB.

 Data packets are transferred from the local area network LAN1 to a destination personal computer PC situated in the local area network LAN3 in a largely similar
30 manner, with the difference that, in this case, the data packets are addressed to the router device R3 directly using the ATM address ATM3. The router device R3

therefore needs to have both protocol conversion functionality and routing functionality.

In the present exemplary embodiment, fictitious MAC addresses are effective only for communication between a router device and the respective address conversion device apparatus connected directly thereto. In this context, a router device and the address conversion device apparatus connected directly thereto form a separate local area network. Hence, the fictitious MAC addresses FIMAC2, FIMAC3 of the address conversion device apparatus A1 can be used independently of the fictitious MAC addresses FIMAC4, FIMAC5 of the address conversion device apparatus A2. In particular, the fictitious MAC addresses FIMAC2 and FIMAC3 used by the address conversion device apparatus A1 can match the fictitious MAC addresses FIMAC4 and FIMAC5 used by the address conversion device apparatus A2. Fictitious MAC addresses can therefore be formed in an address conversion device apparatus or assigned by system administration independently of the fictitious MAC addresses of another address conversion device apparatus.

To allow a router device R1 or R2 to address network devices uniquely using fictitious MAC addresses, these MAC addresses need to be unique within the local area network formed by the router device and the address conversion device apparatus connected directly thereto. In particular, a fictitious MAC address must not match any real or other fictitious MAC address in this local area network. This may be ensured, by way of example, by allocating real MAC addresses of old network devices no longer in use as fictitious MAC addresses. Alternatively, fictitious MAC addresses may be taken from a contingent reserved only for this purpose. Since fictitious MAC addresses can be repeated in different local area networks, this requires the provision of only one contingent within the scope of an appropriate maximum size for a local area network. The measures cited ensure that no conflict arises between a fictitious MAC address and a real MAC address even when real MAC addresses are changed within the local area network; e.g. ~~on account of~~ due to a network module being replaced.

Abstract Although the present invention has been described with reference to specific embodiments, those of skill in the art will recognize that changes may be

made thereto without departing from the spirit and scope of the invention as set forth in the hereafter appended claims.

Method and device ABSTRACT OF THE DISCLOSURE

5 ~~A method and apparatus~~ for transmitting data ~~wherein it is~~ The invention
makes it possible to transmit data on the basis of hardware addresses from a source
network device (R1) to a destination network device(A2). The source network device
10 (R1) assigns the data to be transmitted a fictitious hardware address (FIMAC2) which
is used to identify a transmission destination without matching the latter's real
hardware address (MAC2) prescribed by the manufacturer. The fictitious hardware
address (FIMAC2) is transferred to an inventive address conversion ~~device (A1)~~
apparatus in which the fictitious hardware address (FIMAC2) has been assigned an
10 address information item (ATM2) identifying the destination network device(A2).
The address information item (ATM2) associated with the fictitious hardware address
(FIMAC2) is then assigned to the data, which are forwarded to the destination network
device (A2) using this address information item(ATM2).

2/PRTS

10/01827Z

GR 99 P 2035

JCO5 Rec'd PCEFTS 13 DEC 2001

Description

Method and device for transmitting data

- 5 The invention relates to a method for transmitting data from a source network device to a destination network device. The invention also relates to an address conversion device for implementing the method. In this context, network devices can be understood to mean
- 10 network nodes in a communication and/or data network, router devices, network modules, networked personal computers and other communication and data processing devices which can be coupled to a network.
- 15 In order to switch data quickly within a network, the data are frequently transmitted in the form of data packets provided with a hardware address as destination address. Hardware addresses, which are also referred to as MAC addresses (medium access control), are addresses
- 20 which are used in the data link layer (layer 2) of the OSI reference model and with which network devices - usually network modules - are provided by the manufacturer. The hardware address for a network device is stored permanently, i.e. unalterably, in the network
- 25 device and is unique throughout the world.

Switching data packets on the basis of hardware addresses is usual, particularly in local area networks ("LANs"). A data packet which is provided with a

30 hardware address for a destination network device and is sent to a LAN is recognized by the destination network device in question as being addressed to it from the hardware address, and is therefore received for further processing or forwarding. Normally,

35 hardware addresses are used only for addressing network devices within a local area network. If a transmission destination is situated outside the local area network, the data packets are generally transported to a router device for the local area network, which router device

1001827Z 13 DEC 2001

transfers the data packets using a network address which is additionally contained in said data packets and identifies the transmission destination. Unlike a hardware address, a network address is resident above the data link layer and can be reversibly assigned to a network device by means of system administration. The network addresses used are frequently "Internet Protocol addresses", also referred to as "IP" addresses below. The router device evaluates the network address in the data packets and, on the basis of this, determines an address information item identifying a destination network device which is registered in the router device and is as close as possible to the transmission destination or is possibly identical thereto. The data packets are then transferred to this destination network device using the address information item. If this destination network device does not match the ultimate transmission destination, this destination network device is responsible for transferring the data packets toward the transmission destination.

A method allowing data packets provided with an IP address to be transferred transparently via an ATM network (ATM: asynchronous transfer mode) to a transmission destination which is coupled to the ATM network and is identified by the IP address is known by the name IpoA (IP over ATM), for example. In this context, a router device uses the IP address in the data packets to determine the ATM address of an ATM exit network node which is as close as possible to the transmission destination and is used to forward the data packets in the ATM network. Aspects of this method are described in Internet specification RFC 2225, for example.

However, the evaluation of IP addresses for alternate routing which these methods require is a relatively complex operation which can generally be implemented

GR 99 P 2035

- 2a -

only with a high level of circuit complexity.

1004327-434301
TOP SECRET

It is an object of the present invention to specify a method for transmitting data from a source network device to at least one destination network device which requires less complex address evaluation. It is also an
5 aim to specify an address conversion device for implementing the method.

This object is achieved by a method having the features of patent claim 1 and by an address conversion device
10 having the features of patent claim 10.

The inventive method conveys data from a source network device to a destination network device using a fictitious hardware address associated with these data
15 as destination address in the source network device. In this context, the switching on the basis of hardware addresses means that no complex evaluation of network addresses, such as IP addresses, is necessary. The fictitious hardware address referred to in this context
20 is a hardware address information item which the source network device uses, on the basis of a transfer protocol used, to identify a transmission destination without matching the latter's hardware address prescribed by the manufacturer - also referred to below
25 as the real hardware address. To be able nonetheless to transfer data associated with a fictitious hardware address to the intended destination network device, an inventive address conversion device is provided. In the latter, fictitious hardware addresses are associated
30 with a respective address information item which identifies a respective destination network device and can be used to convey the data to the respective destination network device.

35 The direct association between fictitious hardware addresses and address information items identifying destination network devices in the address conversion device allows an address information item to be determined very easily, e.g. by accessing an

1001827 12304

association table, using a fictitious hardware address. By contrast, it would be much more difficult to determine such an address information item using an IP address instead of the fictitious hardware address.

5 Since an IP address refers to a transmission destination at the end of a transfer chain, and, in principle, any device provided with an IP address could be addressed throughout the world, there is no point in assigning IP addresses to destination network devices
10 directly. By contrast with this, the number of fictitious hardware addresses to be managed by an inventive address conversion device is limited by the fact that fictitious hardware addresses are provided only for the purpose of addressing transmission
15 destinations registered in the source network device, so that fictitious hardware addresses can be directly assigned to address information items for destination network devices with little memory requirement.

20 A fundamental advantage of the invention is that data can also be conveyed, on the basis of hardware addresses, to destination network devices situated outside the local area network of the source network device. To this end, the source network device needs to
25 assign such a destination network device a fictitious hardware address, which the address conversion device in turn assigns an address information item which can be used to convey the data to the destination network device even outside the local area network of the
30 source network device. This significantly extends the range of application for hardware-address based addressing of network devices.

Another fundamental advantage of the invention can be
35 seen in that changing a real hardware address for a network device, e.g. when replacing a network module, at most requires little reconfiguration effort. This is essentially a consequence of using fictitious hardware addresses. Since these

10018277.12.1304

do not need to match any real hardware address for a destination network device, fictitious hardware addresses can also be retained when real hardware addresses are changed. By contrast with this, in the case of the current prior art, any change to a real hardware address for a network device requires that the hardware address tables be updated for all network devices which are meant to be able to address the altered network device using its hardware address.

Advantageous embodiments and developments of the invention are specified in the subclaims.

The address information item associated with a fictitious hardware address in the address conversion device may advantageously be a real hardware address for the destination network device, e.g. the latter's MAC address prescribed by the manufacturer. Data which are associated with a real hardware address and are transferred to the destination network device are recognized by the latter as being addressed to it and are received for the purpose of further processing or forwarding. If the real hardware address of the destination network device changes, e.g. on account of a network module being replaced, it is necessary only to change the association between real and fictitious hardware addresses in the address conversion device in order to be able to address the destination network device using the unaltered fictitious hardware address.

Alternatively, the address information item assigned to the data may also be a network address - for example an IP address or an ATM address - for the destination network device. Such a network address also allows addressing of destination network devices which are situated in a different communication network than the source network device.

In accordance with one advantageous development of the invention, one or more fictitious hardware addresses to be used as destination address can be formed by the address conversion device and transmitted to the source
5 network device. In this context, fictitious hardware addresses need to be formed such that they are unique in the local area network comprising the source network device and the address conversion device and also do not match any real hardware address in this local area
10 network.

In accordance with another advantageous development of the invention, an enquiry from the source network device after a hardware address for a network device
15 identified by an address information item contained in the enquiry, e.g. an IP address, can be answered by the address conversion device on behalf of the network device in question. Such enquiries may be made, for example, under the "ARP protocol" (address resolution
20 protocol). For this purpose, the address conversion device transmits a fictitious hardware address associated with this address information item in the address conversion device to the enquiring source network device. This is a simple way of entering
25 fictitious hardware addresses into a hardware address table, used for hardware addressing, associated with the source network device. The fictitious hardware addresses entered are then used for all subsequent data transmissions.

30
In accordance with one advantageous embodiment of the invention, the data to be transferred can be transmitted from the source network device to the destination network device via the address conversion
35 device. This means that the address information item to be used to forward the data to the destination network device can be assigned to the data actually in the address conversion device. In addition, the data can be converted in the address conversion device in

T001B27.1.001

GR 99 P 2035

- 6a -

line with a transfer protocol used by the destination
network

100137 13191

device. This means that the source network device requires no functionality going beyond the framework of conventional hardware-address based data transmission in order to perform data transmission in accordance
5 with the invention. The source network device need merely be connected to an inventive address conversion device which can address the destination network device. This allows, by way of example, conventional
10 router devices designed for connecting local area networks directly to be connected to an external communication network, and hence to be coupled to one another, via a respective inventive address conversion device.

15 An exemplary embodiment of the invention is explained in more detail below with reference to the drawing.

In the drawing,

20 figure 1 shows a schematic illustration of three local area networks coupled via an ATM network, and

figure 2 shows a schematic illustration of two address conversion devices.

25 Figure 1 is a schematic illustration of three local area networks LAN1, LAN2 and LAN3 coupled via an ATM network ATM. The local area networks LAN1, LAN2 and LAN3 each comprise a plurality of personal computers
30 PC, PCA, PCB coupled locally by means of Ethernet or FDDI (fiber distributed data interface), for example, and are respectively coupled to the ATM network ATM via a router device R1 or R2 or R3. Whereas the router device R1 for the local area network LAN1 and the
35 router device R2 for the local area network LAN2 are respectively connected to the ATM network ATM via an address conversion device A1 or A2, the router device R3 for the local area network LAN3 is connected to the ATM network ATM directly. The router devices R1 and R2

1001827.121301

are conventional router devices which are actually designed for connecting local area networks directly. By contrast, its direct connection to the ATM network ATM means

2001827 121901

that the router device R3 needs to have not only conventional router functionality but also means for protocol conversion between a transfer protocol used in the ATM network ATM and a transfer protocol used in the local area network LAN3. The router devices R1, R2 and R3 and also the address conversion devices A1 and A2 are considered to be special embodiments of network devices within the context of the exemplary embodiment.

The router devices R1 and R2 have been assigned a respective MAC address MAC1 and MAC2 as real hardware address by the manufacturer and have been assigned a respective IP address IP1 or IP2 by system administration, in the order specified. The router device R3 has an associated IP address IP3 and, in addition, an ATM address ATM3 as network address. The address conversion devices A1 and A2 also have a respective associated ATM address ATM1 or ATM2 as network address. In addition, the personal computer PCB has the associated IP address IPB. The router devices R1, R2 and R3, the address conversion devices A1 and A2 and also the personal computer PCB are respectively uniquely identified by the respectively associated addresses MAC1, MAC2, IP1, IP2, IP3, IPB, ATM1, ATM2 and ATM3.

Figure 2 shows a schematic illustration of the address conversion devices A1 and A2 via which the router devices R1 and R2 are coupled to the ATM network ATM. The address conversion devices A1 and A2 each contain, as functional components, a central controller ZS comprising a protocol conversion device PU, an address assignment device AZ, an address determination device AE and an address checking device AP, and also an association table memory ZT which can be accessed by the central controller ZS. In both address conversion devices A1 and A2, the protocol conversion device PU and the address assignment device AZ, and the address determination device AE and the address checking device

GR 99 P 2035

- 8a -

AP, are respectively produced in a joint module.

1001937 121901

In this exemplary embodiment, the association table memories ZT in the address conversion devices A1 and A2 each contain at least three entries, in accordance with the number of local area networks LAN1, LAN2 and LAN3 coupled. The association table memory ZT in the address conversion device A1 contains

a first entry with the IP address IP1, the MAC address MAC1 and the ATM address ATM1,

a second entry with the IP address IP2, a fictitious MAC address FIMAC2 and the ATM address ATM2, and also a third entry with the IP address IP3, a fictitious MAC address FIMAC3 and the ATM address ATM3.

The association table memory ZT in the address conversion device A2 correspondingly contains

a first entry with the IP address IP2, the MAC address MAC2 and the ATM address ATM2,

a second entry with the IP address IP1, a fictitious MAC address FIMAC4 and the ATM address ATM1, and also a third entry with the IP address IP3, a fictitious MAC address FIMAC5 and the ATM address ATM3.

In this context, the elements of each entry are respectively stored associated with one another.

The fictitious MAC addresses FIMAC1, FIMAC2, FIMAC4 and FIMAC5 each have the format of a hardware address. The fictitious MAC address FIMAC2 or FIMAC3 is used by the router device R1 to address the router device R2 or R3, and the fictitious MAC address FIMAC4 or FIMAC5 is used by the router device R2 to address the router device R1 or R3. To this end, the fictitious MAC addresses FIMAC2, FIMAC3 are entered into a routing table (not shown) for the router device R1, and the fictitious MAC addresses FIMAC4, FIMAC5 are entered into a routing table (not shown) for the router device R2. The fictitious MAC addresses FIMAC1, FIMAC2, FIMAC4 and FIMAC5 are fictitious insofar as they match none of the real hardware addresses MAC1 and MAC2, prescribed by the manufacturer, of the router devices R1 and R2 which they address, or they are not based

on any real hardware address - as in the case of the router device R3. Nevertheless, the fictitious MAC addresses are treated as real MAC addresses from the point of view of the router devices R1 and R2.

5

The fictitious MAC addresses FIMAC2, FIMAC3 and FIMAC4, FIMAC5 are entered into the routing tables for the router devices R1 and R2 by the address conversion devices A1 and A2 under the "ARP" protocol (address resolution protocol). Under this ARP protocol, enquires from the router device R1 or R2 after MAC addresses for network devices are answered by the address conversion device A1 or A2 on behalf of these network devices. In the course of such a request, the enquiring router device R1 or R2 transfers an IP address to the connected network devices with the order to send the MAC address of the network device identified by the IP address to the router device R1 or R2, if known. By way of example, such an enquiry after the MAC address of the router device R2 identified by the IP address IP2 may be transmitted from the router device R1 to the address conversion device A1. In such a case, the address conversion device A1 first checks whether the IP address transferred with the enquiry, in this case IP2, is held in the association table memory ZT. If it is, the enquiry is answered by the address conversion device A1 by sending the MAC address associated with this IP address in the association table memory ZT, in this case the fictitious MAC address FIMAC2, to the enquiring router device R1. The fictitious MAC address FIMAC2 transmitted to the router device R1 is then entered by the router device R1 into its routing table as MAC address for the router device R2. Enquiries from the router device R2 are answered by the address conversion device A2 in a similar manner.

1001927 121301

The fact that such enquiries are answered on a delegated basis by fictitious MAC addresses FIMAC2, FIMAC3 and FIMAC4, FIMAC5 stored in the address conversion devices A1 and A2 means that the real hardware addresses MAC1, MAC2 no longer need to be obtained in a complex manner via the communication network ATM. It also becomes unnecessary for each change to a real hardware address for a router device coupled via the ATM network ATM, e.g. as a result of a network module being replaced, also to involve the routing tables for all other router devices being updated.

The text below considers data being conveyed on the basis of hardware addresses between the local area networks LAN1, LAN2, LAN3 using the example of data transmission from the local area network LAN1 to the local area network LAN2.

To transmit data from the personal computer PCA situated in the local area network LAN1 to the destination personal computer PCB situated in the local area network LAN2, the data are transmitted to the router device R1 in the form of data packets containing the IP address IPB of the destination personal computer PCB. The router device R1 uses the routing table it contains to ascertain that the destination personal computer PC2 identified by the IP address IPB can be reached via the router device R2. Consequently, the router device R1 provides the data packets to be transmitted with the fictitious MAC address FIMAC2 obtained from the address conversion device A1 as the hardware address for the router device R2. The IP address IPB of the destination personal computer PCB is maintained unaltered in the data packets in this context. The data packets are then forwarded from the router device R1 to the address conversion device A1.

In the address conversion device A1, the address

1001827 121301

GR 99 P 2035

- 11a -

checking device AP first checks whether the fictitious
MAC address FIMAC2 received is held in the association
table memory ZT. If it is, the address determination
device

100437 2687007

PE determines the ATM address associated with the fictitious MAC address FIMAC2 in the association table memory ZT - in this case ATM2 -, which ATM address identifies that address conversion device A2 via which the router device R2 is coupled to the ATM network ATM. The data packets to be transmitted are then converted by the protocol conversion device PU, in line with the transfer protocol used in the ATM network ATM, into ATM cells to which the ATM address ATM2 is assigned as network address by the address assignment device AZ. The ATM cells are then forwarded to the ATM network ATM and are transferred therefrom to the address conversion device A2 identified by the ATM address ATM2. In this context, the ATM cells may be transferred both via one or more fixed connections (PVC: permanent virtual circuit) and via one or more switched connections (SVC: switched virtual circuit) to be set up as required in the ATM network ATM.

The address conversion device A2 converts the ATM cells into data packets in line with the IP protocol again, said data packets being provided with the real MAC address MAC2 of the router device R2, which is held in the association table memory ZT in this address conversion device A2. The data packets are then forwarded to the router device R2, which recognizes the data packets as being addressed to it from the real MAC address MAC2 associated with them. The router device R2 then forwards the data packets received, after evaluating their IP address IPB, to the destination personal computer PCB identified by the IP address IPB.

Data packets are transferred from the local area network LAN1 to a destination personal computer PC situated in the local area network LAN3 in a largely similar manner, with the difference that, in this case, the data packets are addressed to the router device R3 directly using the ATM address ATM3. The router device

Variable	Mean	SD	Min	Max
Age	34.5	10.2	20	55
Gender	1.2	0.4	1	2
Marital status	1.5	0.5	1	3
Education	12.5	1.5	9	16
Income	1.5	0.5	1	3
Occupation	1.5	0.5	1	3
Health status	1.5	0.5	1	3
Stress level	1.5	0.5	1	3
Life satisfaction	1.5	0.5	1	3
Self-esteem	1.5	0.5	1	3
Resilience	1.5	0.5	1	3
Optimism	1.5	0.5	1	3
Gratitude	1.5	0.5	1	3
Forgiveness	1.5	0.5	1	3
Empathy	1.5	0.5	1	3
Compassion	1.5	0.5	1	3
Kindness	1.5	0.5	1	3
Generosity	1.5	0.5	1	3
Patience	1.5	0.5	1	3
Humility	1.5	0.5	1	3
Modesty	1.5	0.5	1	3
Shyness	1.5	0.5	1	3
Introversion	1.5	0.5	1	3
Neuroticism	1.5	0.5	1	3
Extraversion	1.5	0.5	1	3
Agreeableness	1.5	0.5	1	3
Conscientiousness	1.5	0.5	1	3
Openness	1.5	0.5	1	3
Stability	1.5	0.5	1	3
Emotion regulation	1.5	0.5	1	3
Attention	1.5	0.5	1	3
Memory	1.5	0.5	1	3
Reasoning	1.5	0.5	1	3
Imagination	1.5	0.5	1	3
Intuition	1.5	0.5	1	3
Insight	1.5	0.5	1	3
Wisdom	1.5	0.5	1	3
Knowledge	1.5	0.5	1	3
Skills	1.5	0.5	1	3
Abilities	1.5	0.5	1	3
Interests	1.5	0.5	1	3
Hobbies	1.5	0.5	1	3
Values	1.5	0.5	1	3
Beliefs	1.5	0.5	1	3
Attitudes	1.5	0.5	1	3
Opinions	1.5	0.5	1	3
Preferences	1.5	0.5	1	3
Choices	1.5	0.5	1	3
Decisions	1.5	0.5	1	3
Actions	1.5	0.5	1	3
Behaviors	1.5	0.5	1	3
Reactions	1.5	0.5	1	3
Responses	1.5	0.5	1	3
Interactions	1.5	0.5	1	3
Relationships	1.5	0.5	1	3
Connections	1.5	0.5	1	3
Networks	1.5	0.5	1	3
Communities	1.5	0.5	1	3
Societies	1.5	0.5	1	3
Cultures	1.5	0.5	1	3
Traditions	1.5	0.5	1	3
Customs	1.5	0.5	1	3
Norms	1.5	0.5	1	3
Standards	1.5	0.5	1	3
Practices	1.5	0.5	1	3
Rituals	1.5	0.5	1	3
Beliefs	1.5	0.5	1	3
Attitudes	1.5	0.5	1	3
Opinions	1.5	0.5	1	3
Preferences	1.5	0.5	1	3
Choices	1.5	0.5	1	3
Decisions	1.5	0.5	1	3
Actions	1.5	0.5	1	3
Behaviors	1.5	0.5	1	3
Reactions	1.5	0.5	1	3
Responses	1.5	0.5	1	3
Interactions	1.5	0.5	1	3
Relationships	1.5	0.5	1	3
Connections	1.5	0.5	1	3
Networks	1.5	0.5	1	3
Communities	1.5	0.5	1	3
Societies	1.5	0.5	1	3
Cultures	1.5	0.5	1	3
Traditions	1.5	0.5	1	3
Customs	1.5	0.5	1	3
Norms	1.5	0.5	1	3

In the present exemplary embodiment, fictitious MAC addresses are effective only for communication between a router device and the respective address conversion device connected directly thereto. In this context, a router device and the address conversion device connected directly thereto form a separate local area network. Hence, the fictitious MAC addresses FIMAC2, FIMAC3 of the address conversion device A1 can be used independently of the fictitious MAC addresses FIMAC4, FIMAC5 of the address conversion device A2. In particular, the fictitious MAC addresses FIMAC2 and FIMAC3 used by the address conversion device A1 can match the fictitious MAC addresses FIMAC4 and FIMAC5 used by the address conversion device A2. Fictitious MAC addresses can therefore be formed in an address conversion device or assigned by system administration independently of the fictitious MAC addresses of another address conversion device.

To allow a router device R1 or R2 to address network devices uniquely using fictitious MAC addresses, these MAC addresses need to be unique within the local area network formed by the router device and the address conversion device connected directly thereto. In particular, a fictitious MAC address must not match any real or other fictitious MAC address in this local area network. This may be ensured, by way of example, by allocating real MAC addresses of old network devices no longer in use as fictitious MAC addresses.

Alternatively, fictitious MAC addresses may be taken from a contingent reserved only for this purpose. Since fictitious MAC addresses can be repeated in different local area networks, this requires the provision of only one contingent within the scope of an appropriate maximum size for a local area network. The measures cited ensure that no conflict arises between a fictitious MAC address and a real MAC address

even when real MAC addresses are changed within the local area network, e.g. on account of a network module being replaced.

FOUO 4437007

Patent claims

1. A method for transmitting data from a source network device (R1) to a destination network device (A2), in
5 which

- a) the source network device (R1) assigns the data to be transmitted a fictitious hardware address (FIMAC2) as destination address, the fictitious hardware address being referred to as a hardware address information item which the source network device (R1) uses, on the basis of a transfer protocol used, to identify a transmission destination without matching the latter's hardware address (MAC2) prescribed by the manufacturer,
10
b) the fictitious hardware address (FIMAC2) is transmitted from the source network device (R1) to an address conversion device (A1),
15
c) the address conversion device (A1) checks whether the fictitious hardware address (FIMAC2) transmitted matches a fictitious hardware address (FIMAC2, FIMAC3) stored in a memory of the address conversion device (A1), and, if the result of the check is positive,
20
d) the data are assigned an address information item (ATM2) which is associated with the transmitted fictitious hardware address (FIMAC2) in the address conversion device (A1), identifies the destination network device (A2) and is used to forward the data to the destination network device (A2).
25

30

2. The method as claimed in claim 1, characterized
in that the address information item assigned to the data is a real hardware address for the destination
35 network device.

3. The method as claimed in claim 1, characterized

- 15a -

[illegible]

address (ATM2) for the destination network device (A2).

4. The method as claimed in one of the preceding claims,

5 characterized

in that a fictitious hardware address to be used as destination address is formed by the address conversion device (A1) and is transmitted to the source network device (R1).

10

5. The method as claimed in one of the preceding claims,

characterized

15 in that an enquiry from the source network device (R1) after a hardware address for a network device identified by an address information item contained in the enquiry is answered by the address conversion device (A1) such that

20 the address conversion device (A1) transmits a fictitious hardware address associated with the address information item in question to the source network device (R1).

6. The method as claimed in claim 5,

25 characterized

in that the address information item contained in the enquiry is a network address.

7. The method as claimed in one of the preceding claims,

30 characterized

in that the hardware address used is an MAC address.

8. The method as claimed in one of the preceding claims,

35 characterized

in that the data are transmitted from the source network device (R!) to the destination network device (A2) via the address conversion device (A1), where the

1004827.1-281001

data are assigned the address information item (ATM2)
associated with the transmitted fictitious hardware
address (FIMAC2).

1001837-134304
TOP SECRET

9. The method as claimed in claim 8,
characterized

in that the data are converted in the address
conversion device (A1) in line with a transfer protocol
5 used by the destination network device (A2).

10. An address conversion device (A1) for converting
fictitious hardware addresses (FIMAC2, FIMAC3) into
address information items (ATM2, ATM3) identifying at
10 least one destination network device (A2, R3), where
the fictitious hardware address referred to is a
hardware address information item which a source
network device (R1) uses, on the basis of a transfer
protocol used, to identify a transmission destination
15 without matching the latter's hardware address (MAC2)
prescribed by the manufacturer, having

a) an association table memory (ZT) in which at least
one fictitious hardware address (FIMAC2, FIMAC3) is
stored associated with a respective address
20 information item (ATM2, ATM3) which identifies a
destination network device (A2, R3),
b) an address checking device (AP) for checking whether
a fictitious hardware address (FIMAC2) coming from
the source network device (R1) matches a fictitious
25 hardware address (FIMAC2, FIMAC3) held in the
association table memory (ZT), and
c) an address determination device (AE) for determining
the address information item (ATM2) associated with
a fictitious hardware address (FIMAC2) which comes
30 from the source network device (R1) and is held in
the association table memory (ZT).

11. The address conversion device as claimed in claim
10,
35 characterized by
an address assignment device (AZ) for assigning data
which come from the source network device (R1) and are
associated with a respective fictitious hardware
address to

1004827 4287007

an address information item associated with the respective fictitious hardware address in the association table memory (ZT).

5 12. The address conversion device as claimed in claim 11,
characterized by
a protocol conversion device (PU) for converting the
data coming from the source network device (R1) in line
10 with a transfer protocol used by the destination
network device (A2).

13. The address conversion device as claimed in one of
claims 10 to 12,
15 characterized by
a device for forming fictitious hardware addresses to
be used as destination addresses.

14. The address conversion device as claimed in one of
20 claims 10 to 13,
characterized by
an address resolution device for answering enquiries
from the source network device (R1) after a hardware
address for a network device, which is identified by an
25 address information item contained in the enquiry, by
looking up the fictitious hardware address associated
with said address information item in the association
table memory (ZT) and transmitting it to the source
network device (R1).

30 15. The address conversion device as claimed in one of
claims 10 to 14,
characterized by
means for entering address information items into the
35 association table memory (ZT).

40048974404

FIG 1

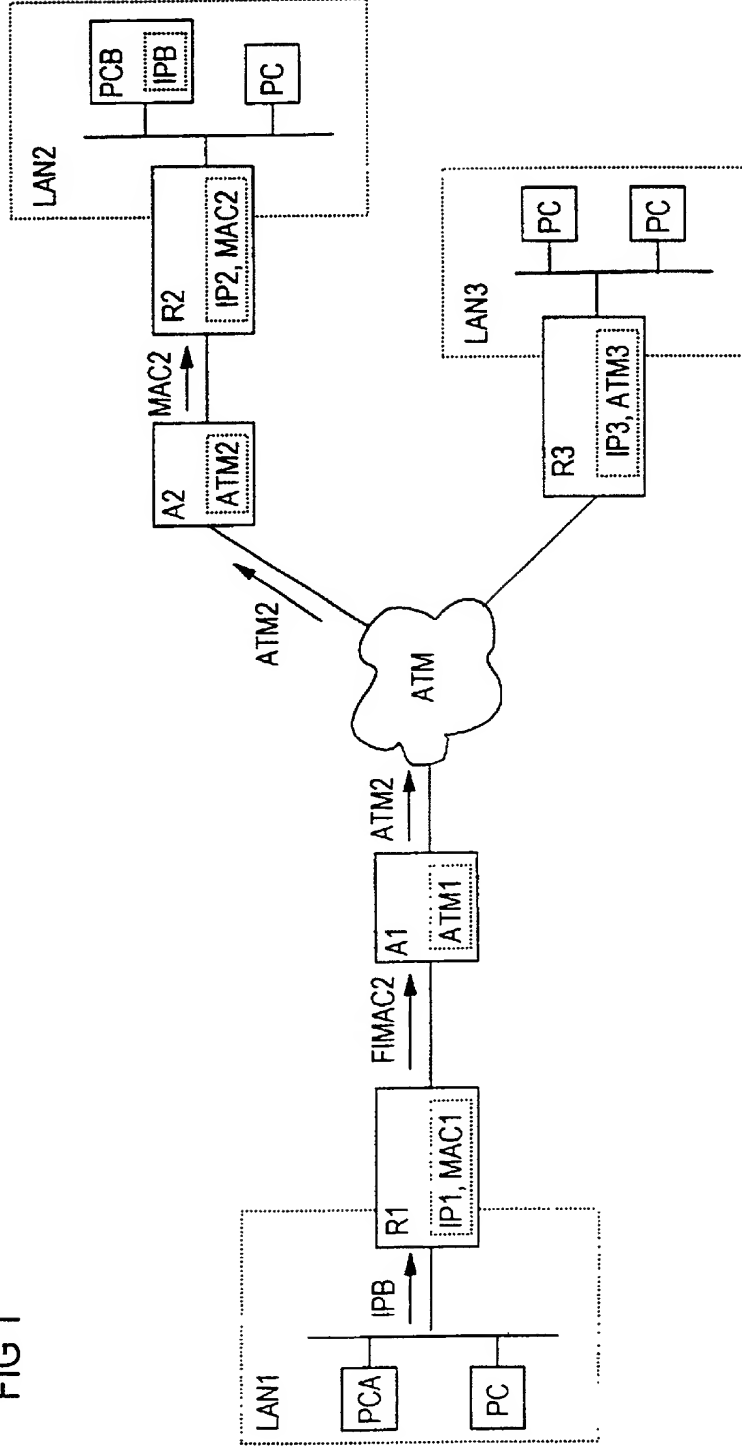
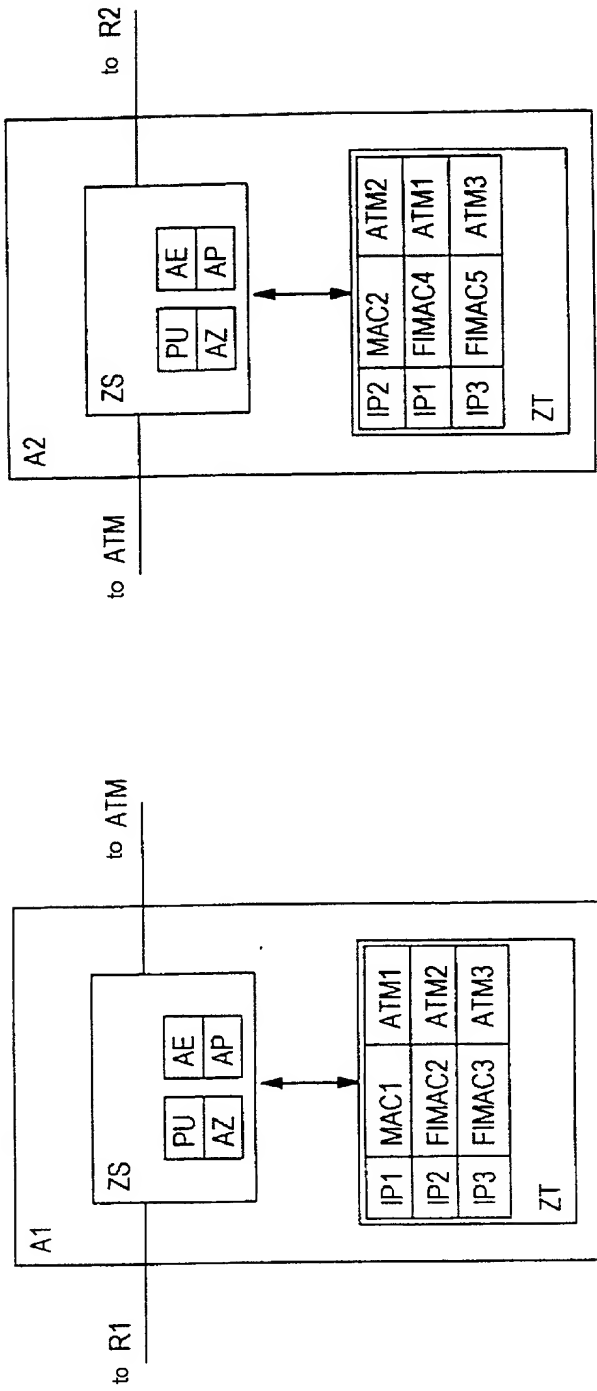


FIG 2



Declaration and Power of Attorney For Patent Application

Erklärung Für Patentanmeldungen Mit Vollmacht

German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Verfahren und Einrichtung zum
Übermitteln von Daten

Method and device for transmitting data

deren Beschreibung

the specification of which

(zutreffendes ankreuzen)

(check one)

☐ hier beigefügt ist

☐ is attached hereto.

☒ am 23.05.2000 als

☒ was filed on 23.05.2000 as

PCT internationale Anmeldung

PCT international application

PCT Anwendungsnummer PCT/DE00/01650

PCT Application No. PCT/DE00/01650

eingereicht wurde und am _____

and was amended on _____

abgeändert wurde (falls tatsächlich abgeändert).

(if applicable)

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign applications
Priorität beansprucht

Priority Claimed

19927304.9

DE

15.06.1999

☒

☐

(Number)
(Nummer)

(Country)
(Land)

(Day Month Year Filed)
(Tag Monat Jahr eingereicht)

Yes
Ja

No
Nein

(Number)
(Nummer)

(Country)
(Land)

(Day Month Year Filed)
(Tag Monat Jahr eingereicht)

☐

☐

Yes
Ja

No
Nein

(Number)
(Nummer)

(Country)
(Land)

(Day Month Year Filed)
(Tag Monat Jahr eingereicht)

☐

☐

Yes
Ja

No
Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

PCT/DE00/01650

(Application Serial No.)
(Anmeldeseriennummer)

23.05.2000

(Filing Date D, M, Y)
(Anmeldedatum T, M, J)

anhängig

(Status)
(patentiert, anhängig,
aufgegeben)

pending

(Status)
(patented, pending,
abandoned)

(Application Serial No.)
(Anmeldeseriennummer)

(Filing Date D,M,Y)
(Anmeldedatum T, M, J)

(Status)
(patentiert, anhängig,
aufgeben)

(Status)
(patented, pending,
abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden können, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

1001827-1300
TOGETHER

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: (Name und Registrationsnummer anführen)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Customer No. 29177

And I hereby appoint

Telefongespräche bitte richten an:
(Name und Telefonnummer)

Direct Telephone Calls to: (name and telephone number)

Ext. _____

Postanschrift:

Send Correspondence to:

Bell, Boyd & Lloyd LLC
Three First National Plaza, 70 West Madison Street, Suite 3300 60602-4207 Chicago, Illinois
Telephone: (001) 312 372 11 21 and Facsimile (001) 312 372 20 98
or
Customer No. 29177

Voller Name des einzigen oder ursprünglichen Erfinders:		Full name of sole or first inventor:	
MICHAEL TIETSCH		MICHAEL TIETSCH	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
<i>Michael Tietsch</i>	2001-11-13		
Wohnsitz		Residence	
KAUFERING, DEUTSCHLAND		KAUFERING, GERMANY DEX	
Staatsangehörigkeit		Citizenship	
DE		DE	
Postanschrift		Post Office Address	
HOEFLEBOGEN 12		HOEFLEBOGEN 12	
86916 KAUFERING		86916 KAUFERING	
Voller Name des zweiten Miterfinders (falls zutreffend):		Full name of second joint inventor, if any:	
Unterschrift des Erfinders		Second inventor's signature	
Datum		Date	
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

FOE at "CAT" - 80